software works seamlessly with any WiMAX Access Service Network Gateway (ASN-GW) device to provide near real-time notifications on the WiMAX network. When power is restored and the WiMAX SmartMeter is re-energized, the SmartMeter automatically scans to find the WiMAX base station. After establishing a link layer connection with the base station, the meter undergoes an initial mutual authentication process via EAP/TLS with the PolicyNet SmartGrid NMS AAA (RADIUS) Server. Upon the successful completion of the mutual authentication process, the WiMAX SmartMeter is granted authorized access to the WiMAX network and secure communications are established between the meter and the base station via the IEEE 802.16.e PKMv2 method. The benefits of this approach are myriad:

a. If any single meter fails, no others are affected (since each meter has a direct connection to the WiMAX base station)
b. Individual device security must be re-validated each and every time the device is powered down (or otherwise disconnected from the WiMAX network), before gaining access to the WiMAX network
c. Notifications and other communications occur in near real-time, affording the utility an up-to-date assessment of its WiMAX Smart Grid network and device status
d. Granular security architecture ensures easy, rapid device identification, isolation and insulation, to ensure overall network security and uptime

5. **WiMAX offers the best of both worlds** – a WiMAX network offers the best of both public and private networks – particularly essential for the Smart Grid (likely the most mission-critical network build-out of the 21st century). WiMAX is government-licensed spectrum (in the U.S., FCC-licensed spectrum is 2300 – 2400 MHz and 2496 – 2690 MHz). Consequently, unlike proprietary mesh networks, which are vulnerable to unrestricted use and "bandwidth hogging" from third-parties (and with no legal recourse to address this problem), WiMAX spectrum is protected by the FCC from unauthorized third-party access. Therefore, by using WiMAX, utilities can depend on uncongested and uncompromised spectrum access on a secure, reliable network infrastructure.

   In addition, a utility can choose to build, control and operate its own virtual private WiMAX network (via spectrum access agreements with WiMAX network services providers, such as Clearwire), or it can choose to sublease network access and associated network services from the WiMAX services provider. In either case, the utility can require guaranteed quality of service (QoS) and other service level agreements (SLAs) from the network services provider, thereby ensuring the performance, bandwidth and security required of its mission-critical Smart Grid network. In the latter case, utilities can benefit from all of the above, but without the operational headaches of managing and maintaining its network internally. Moreover, as a 4G, all-IP network, WiMAX offers significantly higher performance, security, reliability and lower total-cost-of-ownership over competing network architectures (such as proprietary mesh networking).

Conclusion

Utilities require Smart Grid network infrastructure that is reliable, high-performing, cost-effective, scalable and "future proof". WiMAX, a leading fourth-generation (4G), all-IP wireless communications technology, has emerged as a secure, dependable, cost-effective choice for utilities. WiMAX offers utilities an industrial-strength, telecoms-grade communications network infrastructure for Advanced Metering Infrastructure (AMI) and Smart Grid architectures. Its differentiating features include industry-leading, standards-based security, broad territory coverage, exceptional functionality, reliability, performance, cost, and manageability. Equally important, the WiMAX technology roadmap – backed by a large vendor ecosystem in the WiMAX Forum – will continue to support mission-critical utility Smart Grid requirements and innovations into the next generation and beyond.

GRID NET

Policy-Based Network Management

May 2009

340 Brannan Street, #500 San Francisco, CA 94107 t: 415.442.4623 f: 415.442.4628 www.grid-net.com

Executive Summary

Grid Net contends that the best methodology for connecting transmission & distribution (T&D) devices in the Smart Grid is policy-based networking. Well-accepted and broadly deployed throughout the telecommunications industry, policy-based networking has proven itself as the premier means for cost-effective, large-scale, mission-critical network management and monitoring of millions of device endpoints.

As utilities grapple with implementing the Smart Energy Grid, they must find secure, cost-efficient ways to connect and manage a diverse, distributed network of millions of transmission & distribution devices, including (among others) residential and commercial meters, capacitor banks, switches, transformers, and reclosers. This networking challenge is compounded by the following considerations:

- Since the Smart Grid promises to deliver new energy services and capabilities (many of which have yet to be invented), the Smart Grid's network must be both **flexible and adaptable**, to embrace innovation and changing needs over time, while also leveraging legacy T&D infrastructure investments.

- Given the volume of T&D devices to be connected, and the critical importance of monitoring and managing them, the Smart Grid network must be **high-scale**, perform at **high speeds** with **reliability** and **consistency**, and **operate cost-effectively**.

- And while the Smart Grid network holds enormous potential, it also introduces new vulnerabilities; consequently, utilities need to ensure that their Smart Grid networks (and connected devices) are **secure** from network attacks and other network threats, and can perform **reliably** and **resiliently**, even when faced with outages or other unforeseen events.

Policy-based networking offers the best alternative to meet the challenges of the Smart Grid. That's because it enables utilities to apply enterprise policies (business rules) centrally, endowing a distributed network of T&D devices with intelligence (self-management / –reporting capabilities). This combination of 'distributed intelligence' and centralized management delivers exceptional price / performance, as well as the flexibility and adaptability required by the continually-changing needs of the Smart Grid.

Using a policy-based Smart Grid network, utilities can connect and manage T&D devices with a near-real-time, "stateful" (or status-aware) view of all devices in the Smart Grid. Moreover, policy-based networking enables utilities to adapt and deliver new Smart Grid services over time, without having to 'rip out / replace' existing T&D infrastructure.

The Challenge: Networking the Smart Grid

The utility industry faces formidable challenges in connecting transmission and distribution (T&D) devices, in order to form a "smart" energy grid network. The Smart Grid networking challenge is surely one of the largest, most complex of all time, due to a number of factors, including:

- The sheer volume and diversity of T&D devices (in the millions), which are produced by multiple vendors, with a diversity of functions and capabilities, and which operate on a variety of different standards and interfaces.
- The need to leverage legacy energy grid infrastructure and investments (and, in some cases, decades-old devices), while accommodating future change and innovation, in the form of new products and services (some of which have yet to be invented).
- The myriad (and to-be-expected) vulnerabilities introduced by networking millions of diverse and geographically distributed energy grid endpoints. Such vulnerabilities include: denial-of-service attacks, eavesdropping, identity theft, etc.
- Extremely demanding cost and performance requirements of the energy grid. In order to satisfy regulatory and end-customer requirements, utilities must implement Smart Grid networks at the lowest possible cost, but which also deliver the highest possible performance and reliability, in order to ensure reliable, consistent energy transmission.

Smart Grid Network Requirements

Consequently, utilities need to implement a Smart Grid network which

- Provides a real-time view of each T&D device's status
- Accommodates the volume, scale and complexity of devices in the utility grid
- Employs utility and other industry standards, so that utilities can benefit from ongoing innovations in the vendor ecosystem
- Leverages proven innovations in adjacent industries, so that utilities can take advantage of these proven methods with confidence
- Enables cost-effective, automated management of Smart Grid devices, thereby reducing the potential for human errors, while increasing speed and overall performance
- Delivers stable, reliable, and secure performance, so that utilities can meet their Smart Grid service delivery obligations
- Can adapt to new technology and service innovations over time, without requiring a "rip out / replace" of existing T&D infrastructure

The Solution: Policy-Based Networking

Well-accepted and broadly deployed throughout the telecommunications industry, policy-based networking has proven itself as the premier means for cost-effective, large-scale, mission-critical network management and monitoring of millions of network endpoints.

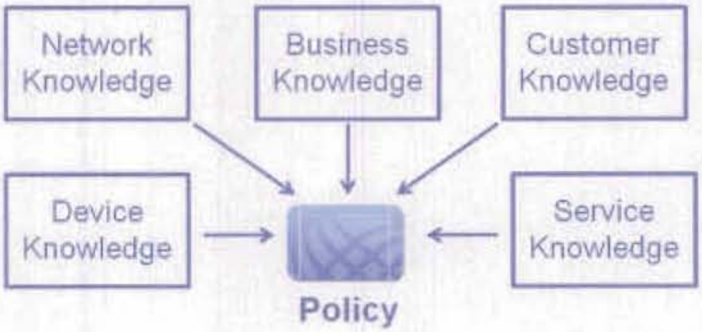
Policy-based networking enables utilities to apply enterprise policies (business rules) centrally, endowing a distributed network of T&D devices with intelligence (self-management / –reporting capabilities). This combination of 'distributed intelligence' and centralized management delivers exceptional price / performance, as well as the flexibility and adaptability required by the continually-changing needs of the Smart Grid.

Using policy-based networking, utilities can connect and manage T&D devices into a Smart Grid network, with a near-real-time, "stateful" (or awareness of devices' status) view of the entire Smart Grid. Moreover, policy-based networking enables utilities to adapt and deliver new Smart Grid policies over time, without having to 'rip out / replace' existing T&D infrastructure, making it exceptionally cost-effective for large-scale network deployments.

What is a Policy?

> *"A policy is a deliberate plan of action to guide decisions and achieve rational outcome(s). Policies differ from* rules *or* law. *While a law can compel or prohibit behaviors (e.g. a law requiring the payment of taxes on income) policy merely guides actions toward those that are most likely to achieve a desired outcome."*[1]

Policies are plans of action that incorporate knowledge across an organization. Policies are defined and implemented, in order to guide an individual's or organization's decisions and to achieve outcomes more expediently.

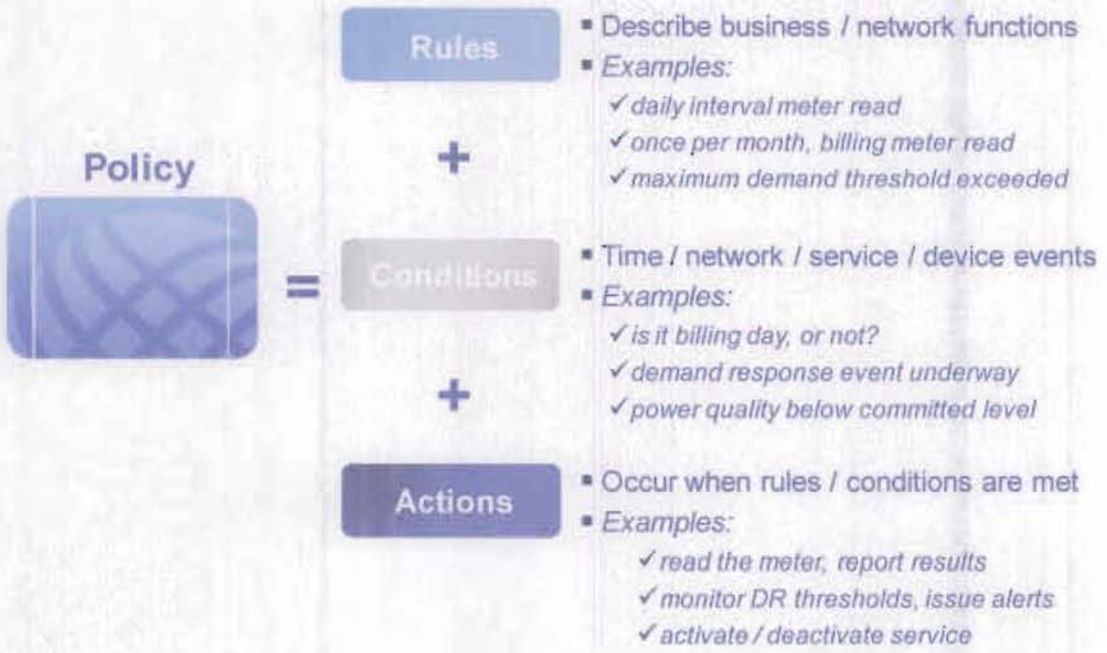


Regarding networks, policies are used to declare and formalize network system behavior. Regarding the Smart Grid, policy-based networking enables a utility to define and manage the system behavior of its Smart Grid network, including: core network capabilities, T&D devices under management, the extent of device "intelligence" and autonomy, and the degrees and types of centrally-enforced controls and governance.

[1] Wikipedia: http://en.wikipedia.org/wiki/Policy

Policies are comprised of rules, conditions and actions, as illustrated below:

Policy Ingredients: Examples in the Smart Grid



Policy = Rules + Conditions + Actions

Rules

- Describe business / network functions
- *Examples:*
  - ✓ *daily interval meter read*
  - ✓ *once per month, billing meter read*
  - ✓ *maximum demand threshold exceeded*

Conditions

- Time / network / service / device events
- *Examples:*
  - ✓ *is it billing day, or not?*
  - ✓ *demand response event underway*
  - ✓ *power quality below committed level*

Actions

- Occur when rules / conditions are met
- *Examples:*
  - ✓ *read the meter, report results*
  - ✓ *monitor DR thresholds, issue alerts*
  - ✓ *activate / deactivate service*

Understanding Policy-Based Network Management (PBNM)

Defined at a deeper level, Policy-Based Network Management (PBNM) systems enable the centralized configuration and control of distributed heterogeneous network resources (e.g., Smart Grid devices) through the systematic definition and application of business rules and procedures.

Policy-Based Network Management systems provide a layer of "abstraction" between business rules (policies) and device-specific configurations, which enable a number of key benefits, including:

- Eliminating the error-prone process of manually configuring individual devices or groups of devices

- Simplifying the task of network management, by centralizing the management function, while also empowering Smart Grid devices with agreed-upon policies for more efficient and responsive Smart Grid network behavior

- Scaling Smart Grid network management to millions of "nodes" or T&D devices, through the use of group policies

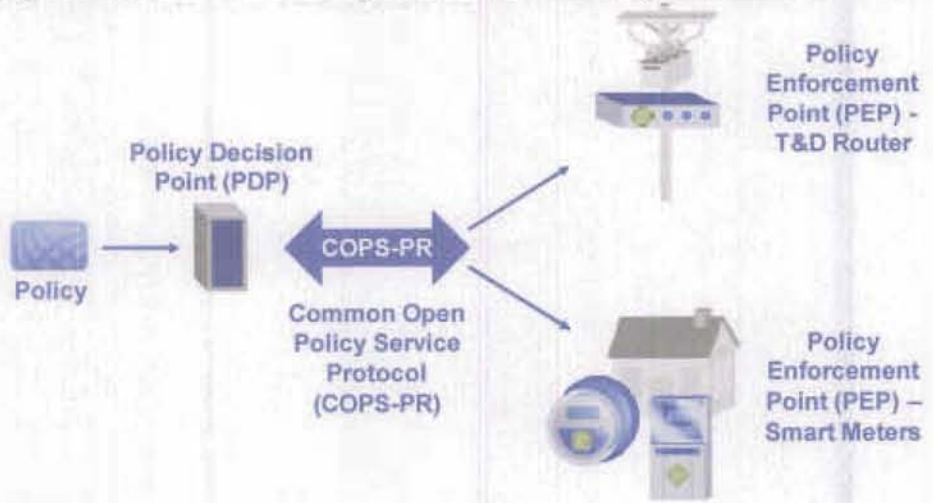
Together, these key benefits confer significant cost efficiencies in network operations, and reduce the Total Cost of Ownership (TCO) of the network.

Key Benefits of Policy-Based Network Management

- *Centralized Configuration and Control*
- *Easy, Intuitive Network Management*
- *Lower Total Cost of Ownership*
- *No Human Intervention Required*
- *Stability and Efficiency*
- *Real-time Error Resolution*

In a policy-based network, there are three important constituents (see figure below):

Key Constituents of Policy-Based Networking in the Smart Grid



- Policies are *maintained* by a **Policy Decision Point** (PDP). The PDP is the policy server (or other logical entity) responsible for: maintaining all policies and their states, for issuing policy decisions, and for providing configuration information in response to requests. This is the "abstraction layer" where policies are translated into device- or application-specific context.
- Polices are *enforced* by a **Policy Enforcement Point** (PEP). All Smart Grid managed elements (e.g., smart meters, routers, capacitor banks, transformers, etc) may function as a PEP element on the Smart Grid network. The PEP is where distributed policy enforcement

takes place. This component may be embedded as part of a smart device (such as a smart meter) or implemented as a proxy to support a "dumb" device (e.g., within a router that is connected to a T&D device).

- The PDP and the PEP are *connected* through use of the **COPS protocol**. COPS (Common Open Policy Service) is a robust, versatile query / response protocol used to exchange policy information between a Policy Decision Point and its Policy Enforcement Points. Created for the general administration, configuration, and enforcement of policies in the telecommunications industry, COPS is designed to be simple yet extensible, so that new kinds of Policy Enforcement Points (e.g., T&D devices) may be supported in the future without changing the protocol. The IETF RFC- 2748 and RFC-3084 are international standards that cover the COPS protocol. COPS provides strong message-level security for authentication, replay protection, and message integrity. COPS can also run over existing Internet security protocols such as IPSec or TLS.

  COPS is "stateful" (e.g., maintains real-time awareness of PEP device status), as follows:

  1. The Request / Decision state is shared between the PDP and the PEP
  2. The state from previous events (Request/Decision pairs) may be inter-associated
  3. COPS also allows the PDP to push configuration information to the PEP, and then allows the PDP to remove such state from the PEP when no longer applicable

Policy Based Networking in the Utility Industry – Some Examples

Utilities have many systems such as Customer Information, Billing, Service Provisioning, Outage Management, Distribution Automation, and Work Management, to name a few. Ideally, all of these systems should be networked to the Smart Grid, and their functionality should be deployed as policies throughout the Smart Grid network, to ensure improved energy service delivery and efficient T&D operations. Below are several examples that illustrate the power and diversity of policy-based networking in utility Smart Grid operations.

Energy service interruptions, service connects / disconnects, customer moves and other manual and / or resource-intensive operational challenges. These activities can be defined as policies and managed in a policy-based Smart Grid network. For example, a manual *Customer connect / disconnect change* is an expensive, error-prone process where customer authentication occurs with web-site interface or via telephone That information is usually retrieved manually, and re-inputted into the utility's Customer Information System (CIS).

In a policy-based network management system, the customer can log into a web-site to request a service change, enter all required information. The utility's Customer Information System (CIS) automatically feeds this disconnect/reconnect information into the PBNM system which fully automates the service change by translating the business processes into policies, which are then distributed to a smart meter (PEP device) and deployed / enforced by the PEP, resulting in significant operational costs savings through greater automation and system integration.

Real-time awareness of Smart Grid outages and failures: For the first time ever, policy-based networking can aid utilities in responding rapidly to Smart Grid failures and outages. In the current electricity grid, a utility must rely on its customers to notify it of Grid outages.

Using policy-based networking in the Smart Grid, the utility's Policy Decision Point server maintains "stateful" awareness (e.g., real-time status awareness) of all connected T&D devices (Policy Enforcement Points). When there is an electricity failure, the affected PEP device (or devices) notifies the Policy Decision Point, which can automatically transmit this information to the utility's enterprise systems, for further rapid action, thereby providing the distributed decision-making capabilities required to operate the Smart Grid at maximum efficiency.

New service offerings: Operations such as tariff changes, load control, demand response, service-disconnect, capacitor bank activation, and power re-routing and restoration can all benefit from policy-based networking. Equally important is the need to accommodate future innovations – which in many cases haven't even been created – without requiring significant new investments over time. For example, utilities are eager to motivate customers to subscribe to new billing services that empower customers to adjust energy usage (while also smoothing demand). At present, changing tariffs records and reprogramming meters is arduous, and usually involves a "truck roll" to implement the change.

Using a policy-based networking system, utilities can define new services as policies, and deploy those policies to subscribing customers (or classes of customers) from a central server, or Policy Decision Point. Once the new billing policy is deployed to the smart meter, the Policy Enforcement Point, it can become activated, with resulting notification sent back over the Smart Grid network, to the Policy Decision Point, and onward to other associated utility systems, such as Customer Billing, CIS, which are automatically updated with the new customer / service activation information. Automating this process results in both operational savings and load-shaping potential for the utility, as well as tangible economic and environmental benefits to customers.

Conclusion: The Many Benefits of Policy-Based Networking in the Smart Grid

Policy-based networking delivers clear benefits to utilities, as follows:

Real-time monitoring and management of the entire Smart Grid network. In the utility's Smart Grid network, PBNM systems are responsible for the efficient management of not just meters, but also generation, transmission, distribution and consumption devices. A policy-based management system manages this complex network by maintaining stateful (e.g., always up-to-date), detailed knowledge of the grid topology and behavior.

Cost-efficient, consistent Smart Grid network performance. By defining policy triage in advance of potential network conditions (e.g., outages), policy-based network systems can provide more rapid, consistent issue resolution, resulting in more cohesive, reliable, consistent network behavior. Efficient network operation translates into lower Total Cost of Ownership (TCO) and improved customer service.

Automated, scalable, adaptable Smart Grid services: Policy-based networking automates the management of distributed policies, such as energy usage data, payment channels, energy quality, service subscriptions, and much more. The PBNM system can manage the vast number of Smart Grid devices, and be flexible enough to scale "horizontally" as load increases, additional devices and / or new services (e.g., new policies) are added over time, to meet utilities" changing business needs.

GRID NET

Appendix

The following IETF RFCs provide more information on policy management.

- RFC 2216 (Network Element Service Specification Template, September 1997)
- RFC 2748 (The COPS (Common Open Policy Service) Protocol, January 2000)
- RFC 2749 (COPS Usage for RSVP, January 2000)
- RFC 2750 (RSVP Extensions for Policy Control, January 2000)
- RFC 2751 (*Signaled Preemption Priority Policy Element, January 2000*) [see RFC 3181]
- RFC 2752 (Identity Representation for RSVP, January 2000)
- RFC 2753 (A Framework for Policy-Based Admission Control, January 2000)
- RFC 2768 (A Report of a Workshop on Middleware, February 2000)
- RFC 2990 (Next Steps for the IP QoS Architecture, November 2000)
- RFC 3052 (Service Management Architectures Issues and Review, January 2001)
- RFC 3060 (Policy Core Information Model-Version 1 Specification, February 2001)
- RFC 3084 (COPS Usage for Policy Provisioning or COPS-PR, March 2001)
- RFC 3181 (Signaled Preemption Priority Policy Element, October 2001, Obsoletes RFC 2751)
- RFC 3198 (Terminology for Policy-Based Management, November 2001)
- RFC 3317 (Differentiated Services QoS Policy Information Base, March 2003)
- RFC 3318 (Framework Policy Information Base, March 2003)
- RFC 3483 (Framework for Policy Usage Feedback for COPS-PR, March 2001)
- RFC 3571 (Feedback Framework Policy Information Base, March 2003)
- RFC 3318 (Policy Core LDAP Schema, February 2004)
- RFC 4261 (Common Open Policy Service Over Transport Layer Security, December 2005)

About Grid Net

Founded in 2006 by Ray Bell, Grid Net (http://www.grid-net.com) is a leading provider of open, interoperable, policy-based network management software, and communications products for the utility industry's Smart Grid. Grid Net's PolicyNet Smart Grid NMS™ comprises a powerful, scalable Smart Grid network control plane that enables the efficient, real-time delivery and management of secure, scalable and high-performing Smart Grid services, including Smart Metering and Distribution Automation.

The Grid Net team brings deep experience from a wide array of industries, including enterprise software, telecommunications, wireless networking, and energy management. With proven track records in technology innovation and product development, we are delivering truly open, standards-based solutions for the Smart Grid.

In 2008, Grid Net licensed its WiMAX SmartMeter and SmartGrid Router products to GE Energy, for use in GE's advanced meter and router product family that is bundled with Grid Net's PolicyNet software.

For more information, please contact Judith McGarry, jhmcgarry@grid-net.com, or (415) 971-2900.

GRID NET

WiMAX Network Resource Management

Copyright

Trademarks

Products as well as other brands and their products within this document are trademarks or registered trademarks of their holders and should be treated as such.

Notice

September 2009

Grid Net, Inc

GRID NET

All Rights Reserved

This notice is intended as a precaution against inadvertent publication and does not imply publication or any waiver of confidentiality. The year included in the foregoing notice is the year of creation of the work.

The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the specific agreement. It is against the law to copy the software on any medium except as specially allowed in the license or nondisclosure agreement. No part of this document may be re-produced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage or retrieval systems, for any purpose other than the licensee's use without the express written consent of Grid Net. The information and/or drawings set forth in this document and all rights in and to disclosing or employing the materials, methods, or techniques described herein are the exclusive property of Grid Net.

Unless otherwise noted, all names of companies, products, street addresses, and persons contained herein are part of a completely fictitious scenario or scenarios and are designed solely to document the use of a Grid Net's product. All company and product names mentioned in this document are the trademark or registered trademarks of their respective companies.

Table of Contents

I. Introduction

To better understand the capabilities and advantages of the WiMAX Smart Grid Solution, one must first understand some of the key features available within WiMAX1. The purpose of this document is to provide utility audiences with a deeper understanding of:

- WiMAX definitions and network overview
- WiMAX network control channels and network connection resources
- Considerations in WiMAX network resource planning

II. The 802.16 WiMAX Standard and Spectrum

IEEE 802.16 is a series of broadband standards authored by the IEEE (Institute of Electrical and Electronics Engineers), for global deployment of broadband metropolitan area networks. WiMAX is the name derived from "Worldwide Interoperability for Microwave Access" and is supported by the WiMAX Forum (http://www.wimaxforum.org), a consortium of more than 500 member organizations whose mission is to promote and certify compatibility and interoperability of broadband products and technologies, based on the IEEE 802.16 standards.

The 802.16 specification applies across a wide swath of the RF (radio frequency) spectrum – some of it government-licensed, and some of it unlicensed – across multiple band ranges and channels. The most popular implementation of the IEEE 802.16 standard is the **802.16e-2005** amendment (mobile WiMAX) that is now in process of being deployed around the world. The 802.16e specification standardizes two aspects of the air interface - the physical layer (PHY) and the Media Access Control (MAC) layer (more information on this, in sections below).

The WiMAX Forum has published three licensed spectrum profiles: 2.3 GHz, 2.5 GHz and 3.5 GHz, in an effort to drive economies of scale. In the U.S., the biggest segment available is around 2.5 GHz, and the FCC (Federal Communications Commission) has granted this spectrum to Clearwire. Elsewhere in the world, the most-likely bands used will be the WiMAX Forum-approved ones, with 2.3 GHz probably being most important in Asia. Since October 2007, the Radio communication Sector of the International Telecommunication Union (ITU-R) has decided to include WiMAX technology in the IMT-2000 set of standards. This enables spectrum owners (specifically in the 2.5-2.69 GHz band at this stage) to use Mobile WiMAX equipment in any country that recognizes the IMT-2000. Some countries in Asia may use a mix of 2.5 GHz, 3.3 GHz and other frequencies.

[1] *IEEE 802.16.e – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*

Analog TV bands (700 MHz) are available for WiMAX usage, but await the complete roll out of digital TV, and there will be other uses for that spectrum (potentially making guaranteed of quality of service in this range a challenge). In the unlicensed band 5.x GHz is the approved profile, although because it is unlicensed, companies are unlikely to use this spectrum widely other than for backhaul, since they do not own and control the spectrum (and therefore cannot guarantee quality of service).

III. WiMAX Network Equipment Types

A WiMAX Access Network is comprised of three main types of network equipment devices, namely the Subscriber Station (SS), the Base Station (BS), and the Access Service Network Gateway (ASN-GW). The Serving BS is the network device to which an SS (e.g., a smart meter) establishes a mutually authenticated and secure air interface network link connection. The ASN-GW is the network device which initiates the network authentication process with the SS, on behalf of the Serving BS, and which maintains the SS's Network Connection Metadata (e.g., Security MSK, Service Flow Configurations, etc.).

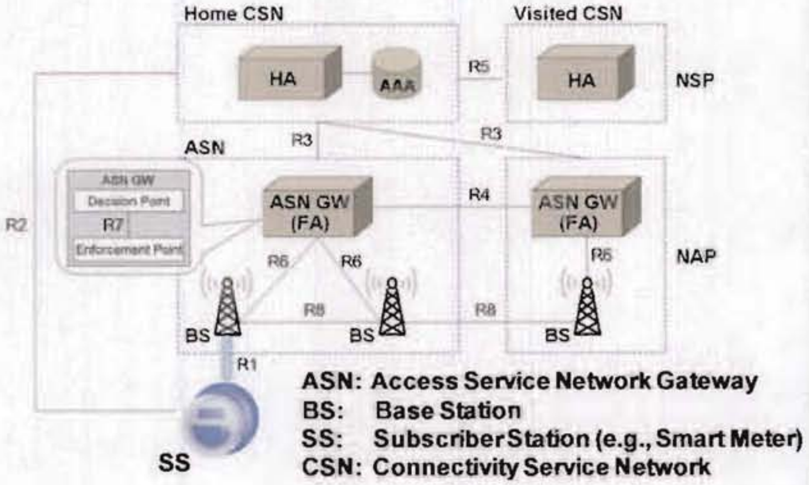


Figure 1 – WiMAX Network Equipment Devices

IV. WiMAX Network Connection Modes

WiMAX has three modes of network connectivity: Normal Mode, Sleep Mode, and Idle Mode:

- ***Normal Mode*** is where the SS has an established DL/UL Channel Connection with the Serving BS, and over which the SS transmits data via the BS's connection scheduling model (i.e., Time Division Duplexing – TDD).

- ***Sleep Mode*** is where the SS can be absent from the Serving BS during pre-negotiated intervals. Before switching to Sleep Mode from Normal Mode, the SS shall inform the BS using a sleep request message (MOB-SLP-REQ) and obtain its approval through a sleep response message (MOBSLP-RSP) from the BS.
- ***Idle Mode*** is where the SS does not need to transmit or receive user data. This mode means the SS is completely deregistered from the Serving BS, freeing up valuable resources from the WiMAX network so that other users can connect to transfer and receive user data. In Idle Mode the ASN-GW maintains the SS's Network Connection Metadata, and the SS will continue to scan the network and keep track of its location, providing a paging update to the network when it moves out of a predefined location or within a defined period of time. This is so the ASN-GW can update the SS location so that the next time it needs to receive data from the network it can be quickly located by the ASN-GW device.

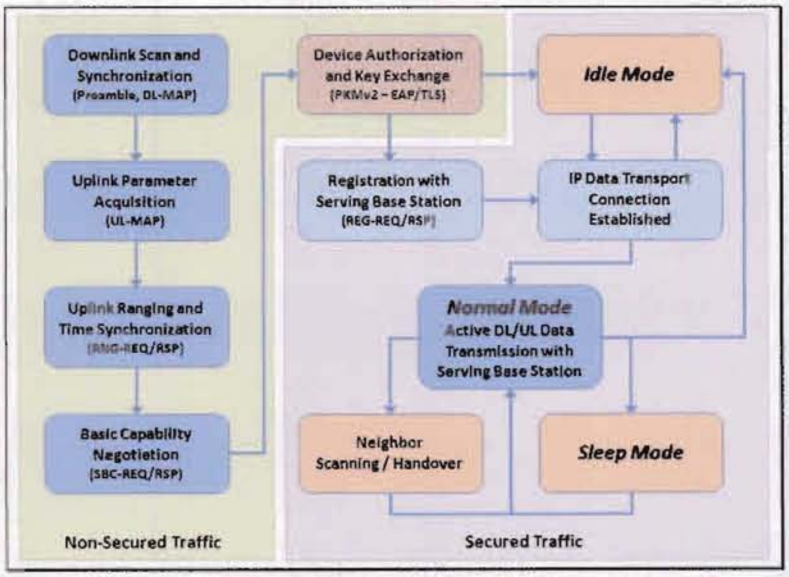

Downlink Scan and Synchronization (Preamble, DL-MAP)
Uplink Parameter Acquisition (UL-MAP)
Uplink Ranging and Time Synchronization (RNG-REQ/RSP)
Basic Capability Negotiation (SBC-REQ/RSP)
Device Authorization and Key Exchange (PKMv2 – EAP/TLS)
Registration with Serving Base Station (REG-REQ/RSP)
Idle Mode
IP Data Transport Connection Established
Normal Mode
Active DL/UL Data Transmission with Serving Base Station
Neighbor Scanning / Handover
Sleep Mode
Non-Secured Traffic
Secured Traffic

Figure 2 – WiMAX Network Connection Process and Modes

V. WiMAX Duplexing Modes

The IEEE 802.16e-2005 standard supports both Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) modes; however, the releases of the WiMAX Forum Profiles to date only include the TDD mode of operation. The TDD mode is preferred for the following reasons:

- It enables dynamic allocation of downlink (DL) and uplink (UL) resources to efficiently support asymmetric DL/UL traffic (adaptation of DL:UL ratio to DL/UL traffic).

- It ensures channel reciprocity for better support of link adaptation, MIMO, and other closed-loop advanced antenna techniques such as transmit beam-forming.
- Unlike FDD, which requires a pair of channels, TDD only requires a single channel for both downlink and uplink providing greater flexibility for adaptation to varied global spectrum allocations.
- Transceiver designs for TDD implementations are less complex and are therefore less expensive (restrictions in the number of DL/UL switching points).

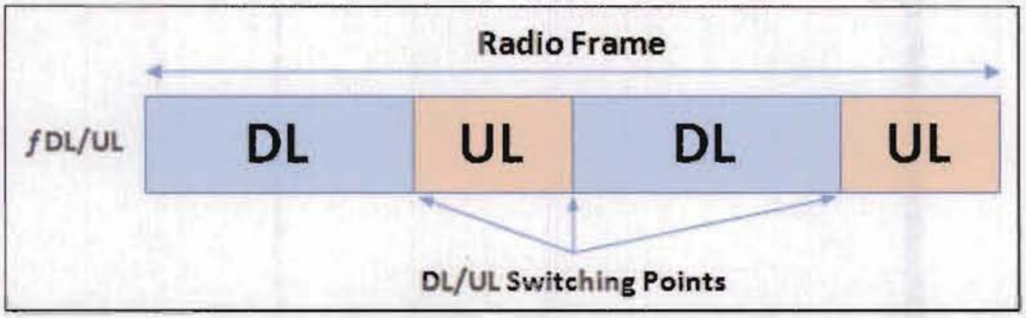


Figure 3 – WiMAX TDD Radio Frame

VI. WiMAX OFDMA

In WiMAX OFDMA (orthogonal frequency-division multiple access), multiple access is two-dimensional (time and frequency). It is important to point out that while a WiMAX Base Station Sector can only support a fixed number of Normal Mode connections (e.g., 256), OFDMA is used to dynamically multiplex a significantly larger number of devices across the available normal mode connections.

- Multiple users use separate subchannels for multiple access
  - Improved capacity
  - Improved scheduling and QoS support
  - Reduced interference (no intra-cell interference)
  - Improved link margin (subchannelization gain)
- Flexible subchannelization
  - Pseudo-random permutation (PUSC) for frequency diversity, or
  - Contiguous assignment (AMC) to enable beamforming
- Scalable structure to support variable bandwidths

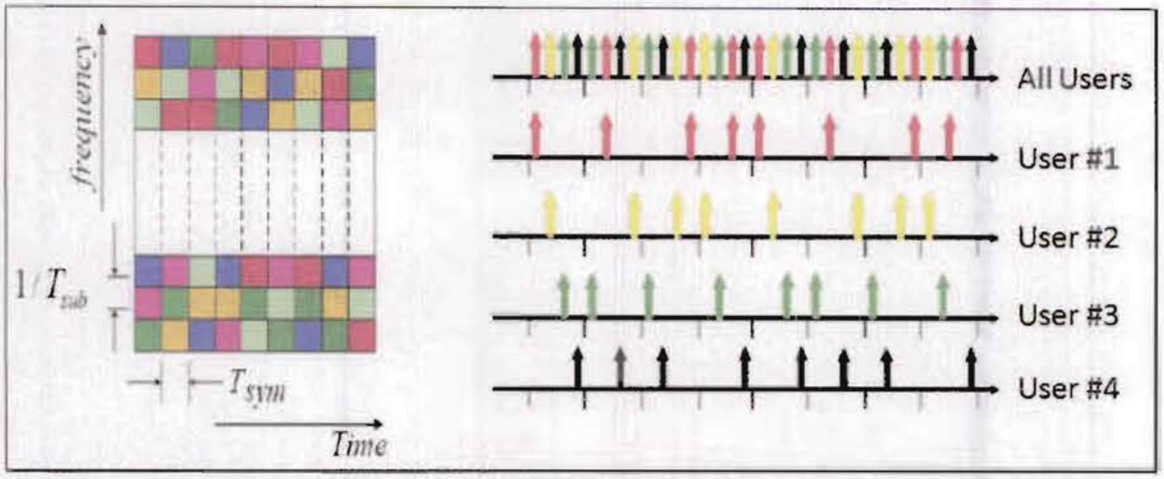


Figure 4 – WiMAX OFDMA Multiple Access

VII. Idle Mode, Multicast/Broadcast, Paging

The SS uses Idle Mode to receive broadcast/multicast service without UL transmission.

- SS associates to broadcast region formed by paging group
- DL traffic received but no UL transmission within broadcast region
- Cell selection may occur but no handover required (no idle mode HO support)
- SS can be paged for DL traffic alerting
- Paging controller in the network coordinates DL traffic and paging
- A SFN network and multi-BS combining is used for Multicast and Broadcast service

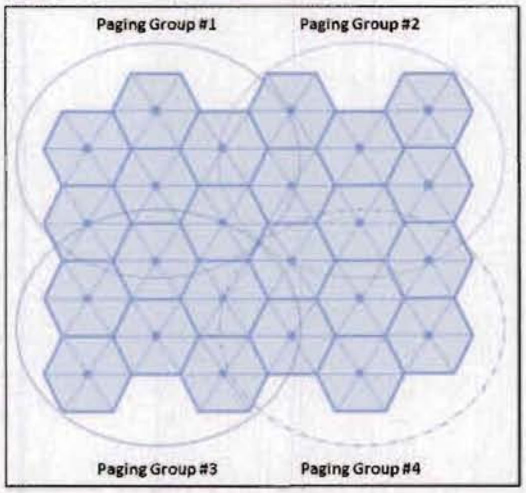


Figure 5 – WiMAX Network Paging Groups

VIII. WiMAX and PolicyNet

Grid Net has developed optimized algorithms and services that facilitate performance of the WiMAX Smart Grid Solution on the WiMAX network. Efforts have focused on exploiting OFDMA technology, optimizing the modes of WiMAX (sleep, idle and normal) and other activities, in order to provide robust, resilient, secure, management access and control of the utility's new digital networked energy points of sale (e.g, the smart meters installed at the customer premise locations), while also helping to deliver the self-healing, self-adaptive secure smart grid network of the future. Grid Net can provide additional information on these optimizations, under NDA, to interested third parties.

GRIDNET

WiMAX SmartGrid Solution Security Overview

Sept 2009

Introduction

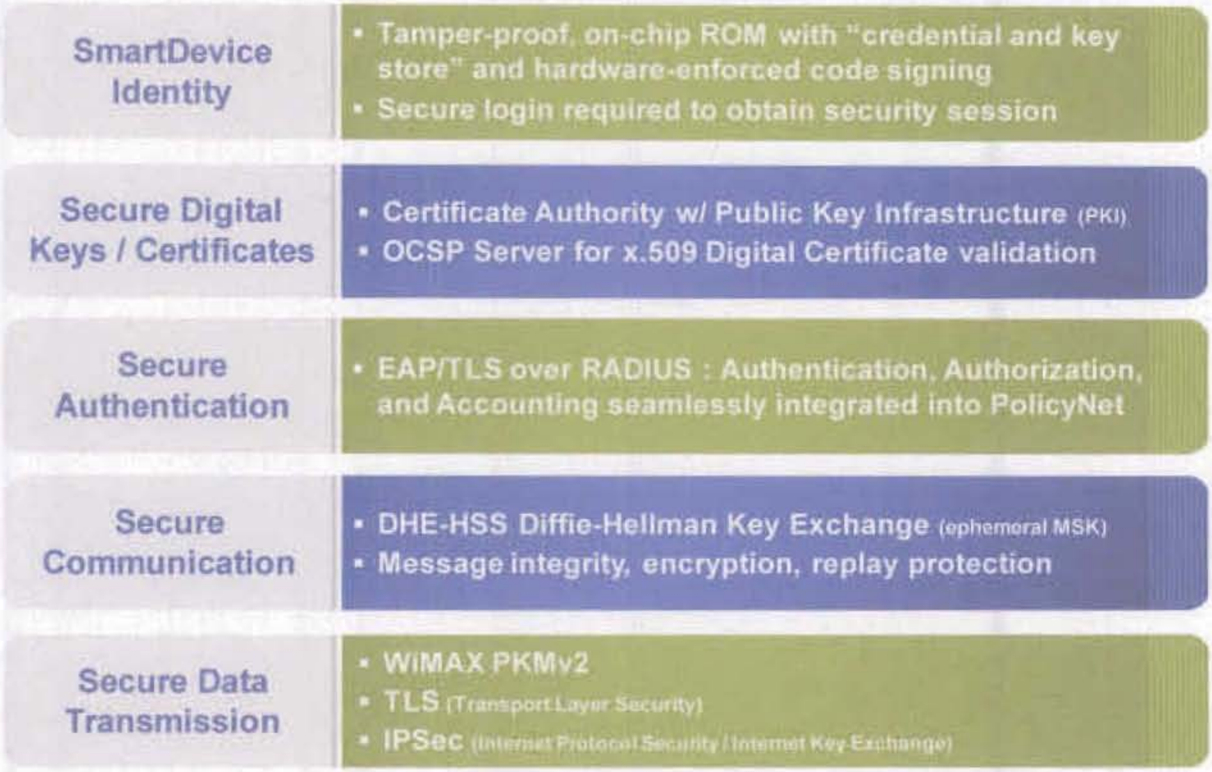
System and network security are of critical concern for any large-scale, mission-critical network infrastructure. Since the Smart Grid is perhaps the most complex, mission-critical network of our time, utilities require Smart Grid technology that is secure, reliable, and self-healing. That's why Grid Net has architected leading security protocols, standards and methodologies into its PolicyNet SmartGrid Network Management System™ (PolicyNet SmartGrid NMS), the industry-leading software suite for management and monitoring Smart Grid networks. It's also why the WiMAX Smart Grid solution contains robust, sophisticated meter security, secure data encryption, and secure data transport via the WiMAX communications network – built with leading security protocols and methods. Moreover, GE and its partner Grid Net are committed to continuous innovation, thereby ensuring that succeeding generations of PolicyNet will contain the latest security enhancements and improvements.

Smart Grid Security Objectives

Grid Net's approach to Smart Grid security is "multi-level / multi-layer" – that is, to architect leading security into Smart Grid devices (WiMAX SmartMeter and SmartGrid Router), into the data, into the PolicyNet Smart Grid network operating system, and into the PolicyNet servers and PolicyNet agents resident in WiMAX SmartGrid Routers and WiMAX SmartMeters. Moreover, the WiMAX Smart Grid solution security architecture supports the cyber security principles of: confidentiality, integrity, availability, identification, authentication, access control, non-repudiation, secure operations, and auditing / accounting.

Multi-Level, Multi-Layer Security Architecture

WiMAX Smart Grid solution's security architecture takes into account the risks associated with all aspects of Smart Grid network activity – including device power-up (or failure and re-energization) and identification, network entry and connectivity, data transport and smart grid network operations. To proactively anticipate points of vulnerability and mitigate risks, the WiMAX Smart Grid solution incorporates leading security methodologies, protocols, algorithms, and standards into the SmartMeter and SmartGrid Router, into device power-up and mutual authentication, authenticity validation, and authorization during smart grid network entry, into data encryption and integrity while in transit or at rest, and into Smart Grid network management, monitoring, and auditing. This "multi-multi" approach is summarized in Figure 1:



SmartDevice Identity	• Tamper-proof, on-chip ROM with "credential and key store" and hardware-enforced code signing • Secure login required to obtain security session
Secure Digital Keys / Certificates	• Certificate Authority w/ Public Key Infrastructure (PKI) • OCSP Server for x.509 Digital Certificate validation
Secure Authentication	• EAP/TLS over RADIUS : Authentication, Authorization, and Accounting seamlessly integrated into PolicyNet
Secure Communication	• DHE-HSS Diffie-Hellman Key Exchange (ephemeral MSK) • Message integrity, encryption, replay protection
Secure Data Transmission	• WiMAX PKMv2 • TLS (Transport Layer Security) • IPSec (Internet Protocol Security / Internet Key Exchange)

Figure 1– Multi-Level/Multi-Layer Approach to Security

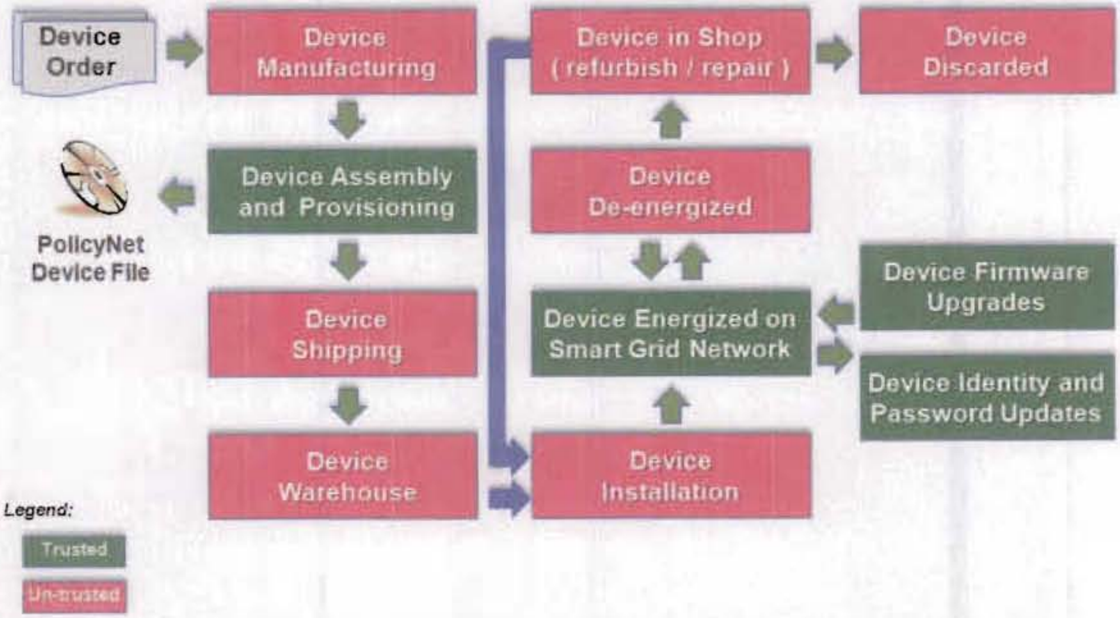


Figure 2 – Overview of Security Lifecycle for WiMAX SmartGrid Devices by GE

Meter Security Implementation, Controls and Validation: "Lifecycle" Approach

During the device assembly process, the GE WiMAX SmartMeter sends a unique "digital signature" (created via the secure ROM chipset on the board with hardware-enforced code signing) that is used to verify the "authenticity" of the meter (i.e., verification that that the meter has not been otherwise physically tampered with after leaving device manufacturing, and that it has no malicious software on board). The WiMAX SmartMeter is then provisioned with a unique pair of WiMAX Forum Certified x.509 Certificates (used for WiMAX Network entry authentication, and for Smart Grid Network entry authentication). The meter utilizes on-board Network Firewall and Intrusion Detection software to protect itself from network level attacks.

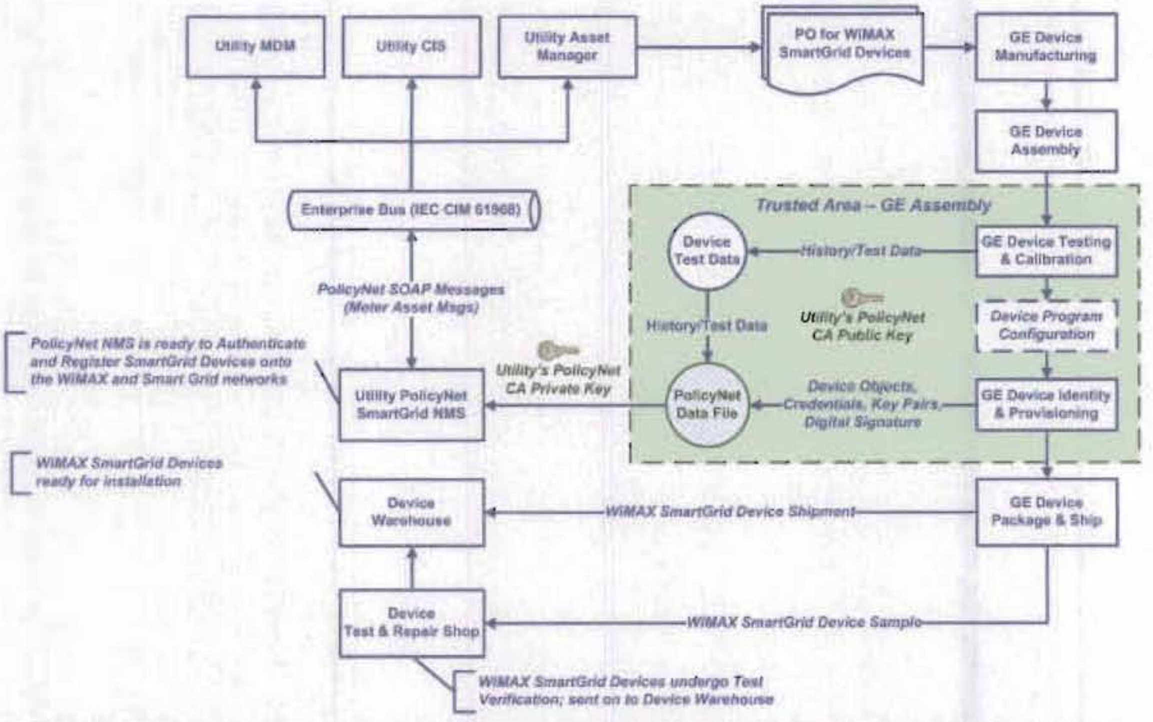

Utility MDM
Utility CIS
Utility Asset Manager
PO for WIMAX SmartGrid Devices
GE Device Manufacturing
GE Device Assembly
Enterprise Bus (IEC CIM 61968)
Trusted Area – GE Assembly
Device Test Data
History/Test Data
GE Device Testing & Calibration
PolicyNet SOAP Messages (Meter Asset Msgs)
History/Test Data
Utility's PolicyNet CA Public Key
Device Program Configuration
PolicyNet NMS is ready to Authenticate and Register SmartGrid Devices onto the WIMAX and Smart Grid networks
Utility's PolicyNet CA Private Key
Utility PolicyNet SmartGrid NMS
PolicyNet Data File
Device Objects, Credentials, Key Pairs, Digital Signature
GE Device Identity & Provisioning
WIMAX SmartGrid Devices ready for installation
Device Warehouse
WIMAX SmartGrid Device Shipment
GE Device Package & Ship
Device Test & Repair Shop
WIMAX SmartGrid Device Sample
WIMAX SmartGrid Devices undergo Test Verification; sent on to Device Warehouse

Figure 3 – Overview of Factory Security Provisioning Process for WiMAX SmartGrid Devices by GE

After a meter is energized, it scans to find the WiMAX network and, after establishing a link layer connection with a base Station, undergoes an initial mutual authentication process via EAP/TLS (using its WiMAX x.509 credentials) with the PolicyNet SmartGrid NMS AAA (RADIUS) Server. Upon the successful completion of the mutual authentication process, the meter is granted authorized access to the WiMAX network and secure communications are established between the meter and the base station via the IEEE 802.16.e PKMv2 method.

Upon the successful mutual authentication process that enables the meter to gain secure access to the WiMAX network, the meter is provided a "quarantined" IP Address that only allows the meter to communicate with a "GateKeeper Process" that is located in a non-routable subnet. The Gatekeeper Process uses a secondary tunneled challenge / response authentication method over TLS that requires the meter to present its unique "digital signature". If the meter's digital signature matches the digital signature created in the factory, then the meter authenticity and meter firmware integrity are proven, and the meter is provided its Smart Grid x.509 Digital Certificate and private/public keys over the TLS connection. At this point, the meter is then provided with a Smart Grid IP Address, and the meter successfully establishes a mutually authenticated and secure connection to the Smart Grid Network (note: any subsequent configuration changes made to the meter, via the PolicyNet software, results in a "new" digital signature being dynamically generated and stored in the PolicyNet Secure Keystore – which is then used for subsequent authenticity validation processes). All subsequent communications between the meter and the PolicyNet software are performed over an encrypted COPS-PR/TLS connection established with the meter's Smart Grid x.509 Certificate and key pair.

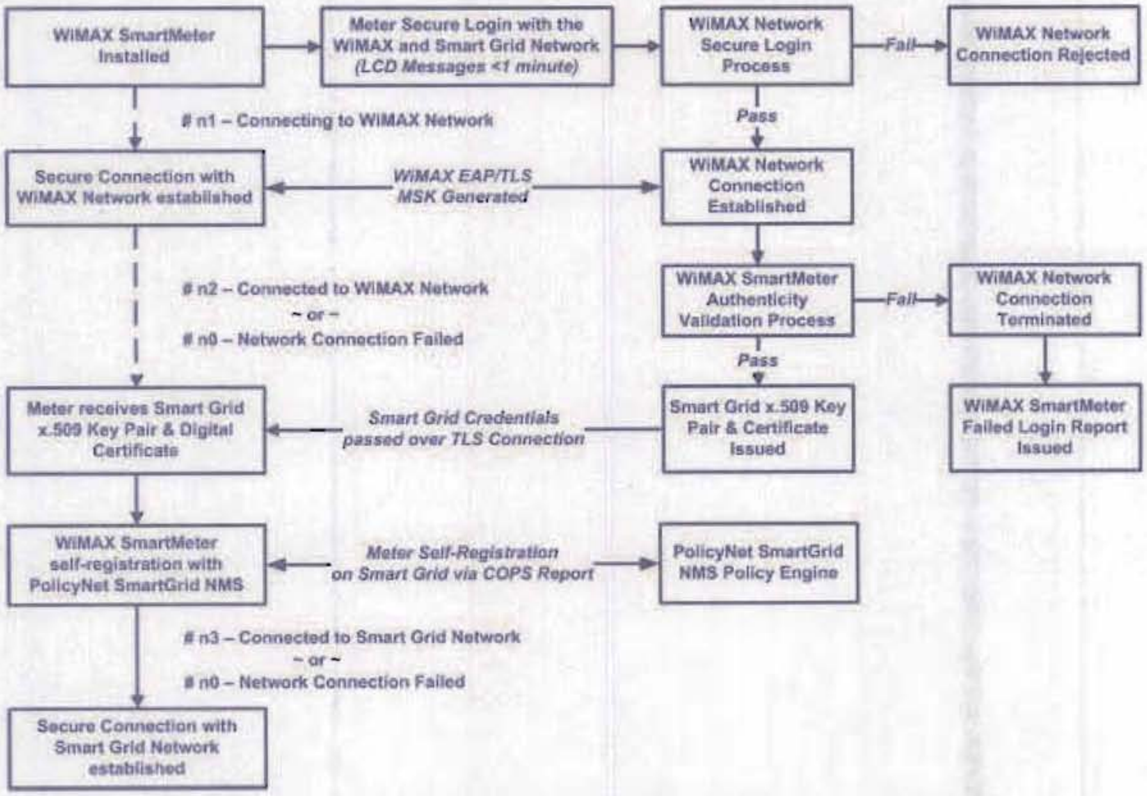

WiMAX SmartMeter Installed
Meter Secure Login with the WiMAX and Smart Grid Network (LCD Messages <1 minute)
WiMAX Network Secure Login Process
Fail
WiMAX Network Connection Rejected
# n1 – Connecting to WiMAX Network
Pass
Secure Connection with WiMAX Network established
WiMAX EAP/TLS MSK Generated
WiMAX Network Connection Established
# n2 – Connected to WiMAX Network
~ or ~
# n0 – Network Connection Failed
WiMAX SmartMeter Authenticity Validation Process
Fail
WiMAX Network Connection Terminated
Pass
Meter receives Smart Grid x.509 Key Pair & Digital Certificate
Smart Grid Credentials passed over TLS Connection
Smart Grid x.509 Key Pair & Certificate Issued
WiMAX SmartMeter Failed Login Report Issued
WiMAX SmartMeter self-registration with PolicyNet SmartGrid NMS
Meter Self-Registration on Smart Grid via COPS Report
PolicyNet SmartGrid NMS Policy Engine
# n3 – Connected to Smart Grid Network
~ or ~
# n0 – Network Connection Failed
Secure Connection with Smart Grid Network established

Figure 4 – Secure SmartGrid Network Entry Process by WiMAX SmartMeter by GE